

Model theory and constructive mathematics

Thierry Coquand

Model theory

A challenge to constructive mathematics

Important results: Ax-Kochen, differential algebraic closure, Mordell-Lang conjecture

Model theory

The starting point of model theory, even the *soundness* theorem, is not effective

Even if we interpret the atomic predicate symbols by decidable predicates the law

$$\forall x.P(x) \vee \exists x.\neg P(x)$$

is not valid intuitionistically

(Solution: *coherent logic*)

Algebraic closure

Another difficulty: not enough models. For instance: algebraically closed field

Field in constructive mathematics: ring (implicitly the addition and multiplication are computable operations) such that $1 \neq 0$ and

$$x = 0 \vee \text{inv}(x)$$

where $\text{inv}(x)$ is $\exists y. 1 = xy$

Any such field is *discrete*: the equality is decidable

Algebraic closure

We cannot decide in general if a polynomial is irreducible or not

$$\forall x. x^2 + 1 \neq 0 \quad \vee \quad \exists x. x^2 + 1 = 0$$

not provable (intuitionistically)

So we cannot in general build the splitting field of $X^2 + 1$

No hope to build the algebraic closure of a field in general

(Possible over \mathbb{Q} or over enumerable field)

Content of the talk

- (1) Quantifier elimination in constructive mathematics, following Herbrand
- (2) Completeness theorem

Example: algebraically closed field

Quantifier elimination

Even soundness of classical first-order logic is problematic constructively

Can we formulate quantifier elimination? What happens?

Herbrand in his thesis presents quantifier elimination from a constructive point of view

Besides soundness, quantifier elimination method seems to use classical equivalence of $\forall x.\varphi$ and $\neg\exists x.\neg\varphi$

Quantifier elimination

Herbrand's example: constant 0 and one function symbol $x + 1$

$$x = x \quad x = y \rightarrow y = x \quad x = y \wedge y = z \rightarrow x = z$$

$$x = y \leftrightarrow x + 1 = y + 1 \quad x + 1 \neq 0$$

$$x \neq x + 1 \quad x \neq x + 2 \quad x \neq x + 3 \quad \dots$$

We write $x + 2$ for $(x + 1) + 1$

Quantifier elimination

Canonical model: \mathbb{N} with all functions computable and atomic predicates decidable

Constructively, this shows the consistency of the theory *without* quantification

A priori, when one looks at compound sentences which use quantifiers it is not decidable anymore

$$\forall x. \exists y. (x + 2 = y + 1 \wedge y = x + 2)$$

Quantifier elimination

The aim of Herbrand was to show the consistency of the theory even with quantifications (not trivial constructively since we cannot rely on the existence of a model)

von Neumann had shown the consistency of the simpler theory

$$x = x \quad x = y \rightarrow y = x \quad x = y \wedge y = z \rightarrow x = z$$

$$x = y \leftrightarrow x + 1 = y + 1 \quad x + 1 \neq 0$$

using Hilbert's ϵ symbol

Quantifier elimination

Key remark: when showing elimination of quantifier for

$$\exists x.\varphi$$

where φ is quantifier free, we show at the same time that this formula is decidable

So we do have $\neg\exists x.\varphi$ equivalent to $\forall x.\neg\varphi$ in a *constructive* way

This is stressed by Herbrand

Quantifier elimination

We get the following result (which is not expressible in a classical framework)

It is possible to compute the truth value of any formula, even if this formula has quantifiers

Any formula is equivalent to a quantifier free formula

The law of classical logic holds for this fragment and the given model \mathbb{N} , and we get that the theory is consistent

Quantifier elimination

This shows that quantifier elimination is interesting from a constructive point of view (even more interesting than classically)

It has been possible for instance to express quantifier elimination for dense linear order (Langford 1927) in intuitionistic type theory (P. Néron, 2009) for the model \mathbb{Q}

C. Cohen and A. Mahboubi have shown in intuitionistic type theory quantifier elimination for algebraically closed fields (2010; the representation is elegant and uses continuations) over the rationals

This method assumes that we have a model (with computable atomic predicates)

Quantifier elimination

Herbrand noticed that quantifier elimination gives a decision procedure (besides a proof of consistency) and conjectured that the method can be used for real closed fields giving a consistency proof for this theory

He adds *mais les méthodes du Chapitre suivant nous y conduiraient plus aisément*, referring to his version of the completeness theorem

We are going to explain this remark for the theory of algebraically closed field (showing the consistency of this theory though we cannot build a model in general)

Completeness Theorem

Proved in the dissertation of Gödel (1929)

The only work of Gödel where he uses non constructive principles (as noticed by J. Avigad)

Use of non constructive reasoning (König's Lemma), besides the non constructive notion of soundness

Completeness Theorem

The introduction of Gödel's 1929 dissertation has a detailed comment on the use of non constructive principle

In particular, essential use is made of the principle of excluded middle for infinite collections (the nondenumerable infinite, however, is not used in the main proof)

It is clear, moreover, that an intuitionistic completeness proof (with the alternative: provable or refutable by counterexamples) could be carried only through the solution of the decision problem for mathematical logic

Completeness Theorem

Herbrand (1929) as a precision of Löwenheim-Skolem, but with a subtle notion of being valid over an infinite domain

Pour que P ne soit pas une identité il faut et il suffit qu'il y ait un champs infini où P soit faux

Herbrand's formulation *only legitimate, similar to the use of ϵ and δ replacing the vague intuition of continuous curve*

Completeness Theorem

Completeness theorem for intuitionistic logic?

Completeness theorem for fragment of classical logic: equational logic and coherent logic

Equational logic the construction of the initial model is constructive and truth in the initial model is the same as provability

Coherent logic where intuitionistic and classical provability coincides. Cut-free proofs have a particularly simple form, described in the paper by M. Coste, H. Lombardi and M.F. Roy, *Dynamical method in algebra*, Ann. Pure Appl. Logic 111 (2001), 203-256

Completeness Theorem, example 1

Classically the intersection of all maximal ideals of a ring is the Jacobson radical which can be described by a first-order formula

$$J(a) = \forall x. \text{inv}(1 - ax)$$

So we have $J(a) \wedge J(b) \rightarrow J(a + b)$

By the completeness result, we should have a direct proof

Completeness Theorem, example 2

Over a local ring, a projection matrix is equivalent to a canonical projection matrix

The statement is first-order and coherent

So classically, we know that we have a direct elementary proof

Completeness Theorem, example 3

Hilbert-Burch theorem

If we have an exact sequence

$$0 \rightarrow R^2 \rightarrow R^3 \rightarrow \langle a_1, a_2, a_3 \rangle \rightarrow 0$$

then the elements a_1, a_2, a_3 have a gcd

This is a statement formulated in a first-order way, but not coherent

$$\exists x. x|a_1 \wedge x|a_2 \wedge x|a_3 \wedge (\forall y. y|a_1 \wedge y|a_2 \wedge y|a_3 \rightarrow y|x)$$

Is there a direct elementary proof? (classically, we know that there is a classical elementary proof)

Completeness Theorem

Completeness theorem for intuitionistic logic

Implicit in Beth's work

Stated and proved explicitly in the 70s by Veldman (Kripke model) and de Swart (Beth model)

Subtle situation: impossible by results of Gödel and Kreisel-Dyson *if* we take the “natural” notion of Kripke/Beth model without “exploding” nodes

Completeness Theorem

Two approaches for classical completeness

(1) Henkin-Lindenbaum

(2) Löwenheim-Skolem-Herbrand-Gödel, gives completeness of *cut-free* proofs

Completeness Theorem

Completeness theorem for coherent logic gives at the same time completeness w.r.t. *cut-free* proofs, using the notion of *site model*

Both a syntactical and a semantical flavour: the “semantics” of a formula is in term of cut-free proof

One shows that the cut-rule is *admissible*

This is actually very close to what Herbrand was doing

Completeness Theorem

For coherent formulae, to be true in a site model means to have a cut-free proof (well-founded tree)

The semantics is sound w.r.t. intuitionistic derivation, and the proof of soundness is similar to a proof of admissibility of the cut-rules

Coherent formulae

$$\varphi(\vec{x}) \rightarrow \exists \vec{y}_1. \varphi_1(\vec{x}, \vec{y}_1) \vee \cdots \vee \exists \vec{y}_n. \varphi_n(\vec{x}, \vec{y}_n)$$

where $\varphi, \varphi_1, \dots, \varphi_n$ are conjunctions of atomic formulae

Simple proof theory (see the work of Coste, Lombardi, Roy)

Site model

Generalisation of the notion of topological model and Beth model

Extracted from Grothendieck's work in algebraic geometry

We limit ourselves to the case of extensions of the theory of rings

Rings form an equational theory, we consider the category of rings

Site model

Elementary covering

local rings $R \rightarrow R[\frac{1}{a}]$ and $R \rightarrow R[\frac{1}{1-a}]$

fields $R \rightarrow R[\frac{1}{a}]$ and $R \rightarrow R/\langle a \rangle$: we force a to be invertible or to be 0

algebraically closed fields: we add $R \rightarrow R[X]/\langle p \rangle$ where p is a monic non constant polynomial

An arbitrary covering is obtained by iterating elementary coverings (in all these cases, we obtain only finite coverings)

Site model

One defines a forcing relation $R \Vdash \varphi$ by induction on φ

$R \Vdash \varphi \rightarrow \psi$ iff for any map $R \rightarrow S$ if we have $S \Vdash \varphi$ then we have $S \Vdash \psi$

$R \Vdash \forall x.\varphi$ iff for any map $R \rightarrow S$ and any element a in S we have $S \Vdash \varphi(a)$

$R \Vdash \exists x.\varphi$ iff we have a covering $R \rightarrow R_1, \dots, R \rightarrow R_n$ and elements a_i in R_i such that $R_i \Vdash \varphi(a_i)$

Site model

$R \Vdash t = u$ iff we have a covering $R \rightarrow R_1, \dots, R \rightarrow R_n$ and $t = u$ in each R_i

We get in this way a model of each coherent theory

For instance we have $R \Vdash \text{inv}(a) \vee \text{inv}(1 - a)$ for the notion of covering associated to local rings

$R \Vdash a = 0 \vee \text{inv}(a)$ theory of fields

$R \Vdash \exists x. x^n + a_1 x^{n-1} + \dots + a_n = 0$ theory of algebraically closed fields

Site model

For algebraic closed fields we have

Lemma: *We have $R \Vdash a = 0$ iff a is nilpotent*

Indeed, if a is nilpotent in $R[X]/\langle p \rangle$ it is nilpotent in R and if a is nilpotent in $R[\frac{1}{b}]$ and in $R/\langle b \rangle$ then it is nilpotent in R

Site model

This model (the “generic” model, similar to the initial model for equational theories) is described in a constructive metatheory

This gives a *constructive consistency* proof for the theory of algebraically closed fields

Indeed $R \Vdash 1 = 0$ iff $1 = 0$ in R

This builds a *generic* model, where the truth-values are non standard

Site model

For the theory of algebraic closure of a field K we need only to consider (0 -dimensional) finitely presented algebra over K

More concretely: each algebra R is given by a finite number of indeterminates x_1, \dots, x_n and polynomial constraints

$$p_1(x_1) = 0, p_2(x_1, x_2) = 0, \dots, p_n(x_1, \dots, x_n) = 0$$

This gives a *computational model* of the algebraic closure of a field, even if we don't have any factorisation algorithm for polynomials over K

One can think of each finitely presented K -algebra as a *finite approximation* of the (ideal) algebraic closure of K

Site model

This is reminiscent of the description of Kronecker's work by H. Edwards

The necessity of using an algebraically closed ground field introduced -and has perpetuated for 110 years- a fundamentally transcendental construction at the foundation of the theory of algebraic curves. Kronecker's approach, which calls for adjoining new constants algebraically as they are needed, is much more consonant with the nature of the subject

H. Edwards *Mathematical Ideas, Ideals, and Ideology*, Math. Intelligencer 14 (1992), no. 2, 6–19.

Site model

This model can be implemented (for instance in Haskell, B. Manna 2010)

This is close to the technique of *dynamic evaluation* of D. Duval (one concrete application: computation of branches of an algebraic curves)

The notion of site model gives a theoretical model of this technique

The same technique can be used for several other first-order theories

M. Coste, H. Lombardi and M.F. Roy, *Dynamical method in algebra*, Ann. Pure Appl. Logic 111 (2001), 203-256

Other theories

It would be interesting to express similarly the theory of *differential algebraic closure*

Our presentation in term of indeterminates with equational forcing conditions is close to the original presentation by J. Drach (1898)

Galois, Liouville and Drach had a similar abstract and formal approach to differential algebra (cf. H. Edwards *Essays on constructive mathematics*)

For instance, they did not think of the elements as analytic functions (for Liouville the theory did not exist yet) but as symbolic elements satisfying some equational constraints

Other theories

“When Galois discussed the roots of an equation, he was thinking in term of complex numbers, and it was a long time after him until algebraist considered fields other than subfields of \mathbb{C} ... But at the end of the century, when the concern was to construct a theory analogous to that of Galois, but for differential equations, they got stuck on the following problem: In what domain do we need to be in order to have enough solutions to differential equations? It was an important contribution of model theory to algebra to answer this question with the notion of *algebraically closed field*... There is no natural example of a differentially closed field.”

Constructively the problem appears already for the algebraic closure of a field

Completeness Theorem

A simple completeness proof for intuitionistic logic for a given theory

Topological model: the truth values are element of a complete Heyting algebra

We have something very like an initial model: the domain is the set of all terms; the Tarski-Lindenbaum algebra is not complete however

We take the Dedekind-MacNeille completion of the Tarski-Lindenbaum algebra of formulae (G. Sambin 1992; there are other possible ways of defining a complete Heyting algebra)

Completeness Theorem

A formula is valid in this model iff it is provable

Hence we have completeness

This completeness result can be as useful as the usual completeness theorem to prove concrete result

Completeness Theorem

Example (J. Smith, Th. C. *An application of constructive completeness* 1995 from an example of Dragalin)

Conservative extension of **HA** where we add a new constant ∞ and a predicate $F(x)$ (x is “feasible”) with axioms

$$F(0) \quad \neg F(\infty) \quad x < y \wedge F(y) \rightarrow F(x)$$

together with the induction principle restricted to F , and closure of F under primitive recursive functions

Other constructive completeness theorem

Church *A Note on the Entscheidungsproblem* JSL 1936 has an errata for the constructive version of his result (proved by Bernays around 1935 using epsilon method)

P. Martin-Löf has a completeness theorem for the \forall, \rightarrow fragment of first-order logic in intuitionistic type theory, using normalisation

Conclusion

The notion of *site model* of a coherent theory gives a constructive proof of completeness which is an elegant way of proving admissibility of cut-free deducibility

The core of many ideas in model theory can be expressed constructively

This formulation may be simpler than the usual formulation, for instance there is no dependence on classical logic and the axiom of choice